

On the distribution of sparse sequences in prime fields and applications

Victor C. García

Departamento de Ciencias Básicas
 Universidad Autónoma Metropolitana–Azcapotzalco
 C.P. 02200, México D.F., México
 vc.garci@gmail.com

Abstract

In the present paper we investigate distributional properties of sparse sequences modulo almost all prime numbers. We obtain new results for a wide class of sparse sequences which in particular find applications on additive problems and the discrete Littlewood problem related to lower bound estimates of the L_1 -norm of trigonometric sums.

2000 Mathematics Subject Classification: 11B39, 11B50, 11L07.

1 Introduction

Throughout the paper $\{x_n\}$ is an increasing sequence of positive integers. The study of distributional properties of the sequence

$$x_n \pmod{p}; \quad n = 1, 2, \dots,$$

and additive problems connected with such sequences are classical questions in number theory with a variety of results in the literature. When $\{x_n\}$ grows rapidly the problem becomes harder for individual moduli, but it is possible to obtain strong results modulo most of the primes p . We mention the work of Banks, Conflitti, Friedlander and Shparlinski [1], where a series of results on distribution of Mersenne numbers $M_q = 2^q - 1$ in residue classes have been obtained. This question has also been considered by Bourgain in [3]. General results on distribution of sequences of type 2^{x_n} , (and generally of the form λ^{x_n}), modulo most of the primes have been obtained by Garaev and Shparlinski [9], and by Garaev [7]. For instance, Garaev [7] has obtained a non-trivial bound for the exponential sum

$$\max_{(a,p)=1} \left| \sum_{n \leq T} e^{2\pi i \frac{a}{p} \lambda^{x_n}} \right|,$$

for $\pi(N)(1 + o(1))$ primes $p \leq N$ and $T = N(\log N)^{2+\varepsilon}$, where $\{x_n\}$ is any strictly increasing sequence of positive integers satisfying $x_n \leq n^{15/14+o(1)}$. Banks, Garaev, Luca and Shparlinski [2] obtained uniform distributional properties of the sequences

$$f_g(n) = \frac{g^{n-1} - 1}{n}, \quad h_g(n) = \frac{g^{n-1} - 1}{P(n)},$$

where g and n are positive integers, n is composite and $P(n)$ is the largest prime factor of n .

Now consider a simpler sequence

$$2^n \pmod{p}; \quad n = 1, 2, \dots$$

From a result of Erdős and Murty [5] it is well-known that 2 has the multiplicative order $t_p \geq N^{1/2+o(1)}$ for $\pi(N)(1 + o(1))$ primes $p \leq N$. Combining this with a result of Glibichuk [11] it follows that for almost all primes p every residue class modulo p can be represented in the form

$$2^{n_1} + \dots + 2^{n_s} \pmod{p},$$

for certain positive integers n_1, \dots, n_s . García, Luca and Mejía [10] have applied similar arguments to obtain analogous results for the sequence of Fibonacci numbers

$$F_n \pmod{p}; \quad n = 1, 2, \dots,$$

where

$$F_{n+2} = F_{n+1} + F_n, \quad n \geq 1,$$

with $F_1 = F_2 = 1$. They proved that for almost all primes p , every residue class modulo p is a sum of 32 Fibonacci numbers.

In the present paper using a different approach we obtain new results on additive properties for general sparse sequences for almost all the prime moduli. In particular we prove that for $\pi(N)(1 + o(1))$ primes $p \leq N$ every residue class is a sum of 16 Fibonacci numbers F_n , with $n \leq N^{1/2+o(1)}$, improving upon the mentioned result of García, Luca and Mejía. Moreover, we establish that for any $\varepsilon > 0$ there is an integer $s \leq 100/\varepsilon$ such that for $\pi(N)(1 + o(1))$ primes, $p \leq N$, every residue class can be written as

$$F_1 + \dots + F_s \pmod{p},$$

with $1 \leq n \leq N^\varepsilon$. We note that the value s has the optimal order $s = \mathcal{O}(1/\varepsilon)$.

From the work of Karatsuba [13] it is known the connection between additive problems and the Littlewood problem on lower bound estimates for the L_1 -norm of exponential sums. Namely, for any coefficients γ_n , $|\gamma_n| = 1$, and any strictly increasing sequence of integers $\{f(n)\}$, Karatsuba established

$$\int_0^1 \left| \sum_{n=1}^N \gamma_n e^{2\pi i \alpha f(n)} \right| d\alpha \geq (N^3/J)^{1/2}, \quad (1)$$

where J denotes the number of solutions of the diophantine equation

$$f(n) + f(m) = f(k) + f(\ell); \quad 1 \leq n, m, k, \ell \leq N.$$

Solving the Littlewood conjecture, Konyagin [14], and McGehee, Pigno and Smith [16] proved that

$$\int_0^1 \left| \sum_{n=1}^N e^{2\pi i \alpha f(n)} \right| d\alpha \gg \log N, \quad (2)$$

where $f(n)$ is an integer valued function. This bound reflects the best possible lower bound in general settings, as it shown by the example $f(n) = n$. However, due to the connection with certain additive problems, for a very wide class of integer valued sequences $f(n)$, estimate (2) has been improved, see, for example, Garaev [6], Karatsuba [13] and Konyagin [15].

Green and Konyagin [12] established a variant of the Littlewood problem in prime fields \mathbb{F}_p . One of their results claims that if \mathcal{A} is a subset of \mathbb{F}_p , with $|\mathcal{A}| = (p-1)/2$, then

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{a \in \mathcal{A}} e^{2\pi i x \frac{a}{p}} \right| \gg (\log p)^{1/3-\varepsilon}.$$

One can use a version of Karatsuba's inequality (1) to get a variety of result for specific sequences. For instance, we employ a recent result of Bourgain and Garaev [4] on additive energy of the set $g^x \pmod{p}$; $1 \leq x \leq N$, and show that for any $N < p^{1/2}$ we have the bound

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right| \gg N^{1/48+o(1)}.$$

For the sequence $\{F_n\}$ of Fibonacci numbers we shall prove the following result: given any positive real $\gamma < 1/3$ there are positive constants $c_1 = c_1(\gamma)$, $c_2 = c_2(\gamma)$ such that for $\pi(N)(1+o(1))$ primes $p \leq N$ the following estimate holds

$$c_1 N^{\gamma/2} \leq \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \leq c_2 N^{\gamma/2}.$$

Acknowledgement. The author is grateful to M. Z. Garaev for sharing his thoughts which has led to the present improvement of the result of [10].

2 Formulation of results

Throughout the paper N and M always denote positive large parameters. Let \mathcal{X} be any subset of $\{1, \dots, 10^M\}$. The first result of our present paper relies on ideas of arithmetic combinatorics.

Theorem 1. *Let $\mathcal{J}(N)$ be the number of solutions of*

$$x \equiv y \pmod{p}; \quad x, y \in \mathcal{X}, \quad p \leq N. \quad (3)$$

The following asymptotic formula holds

$$\mathcal{J}(N) = \pi(N)|\mathcal{X}| + \mathcal{O}\left(\frac{|\mathcal{X}|^2 M}{\log M}\right). \quad (4)$$

Using Theorem 1 we can get the following result on the value set of any sequence modulo most of the primes p .

Theorem 2. *For $\pi(N)(1 + \mathcal{O}(1/\Delta))$ prime numbers $p \leq N$, we have the following asymptotic formula*

$$\#\{x \pmod{p} : x \in \mathcal{X}\} = |\mathcal{X}| + \mathcal{O}\left(\frac{|\mathcal{X}|}{1 + \frac{\pi(N) \log M}{M|\mathcal{X}|\Delta}}\right), \quad (5)$$

where $\Delta = \Delta(N)$ is any function with $\Delta \rightarrow \infty$.

In particular we have the following corollary which can be applied for a large class of sparse sequences.

Corollary 3. *If $M|\mathcal{X}|\Delta^2 \leq \pi(N) \log M$, then*

$$\#\{x \pmod{p} : x \in \mathcal{X}\} = |\mathcal{X}| (1 + \mathcal{O}(\Delta^{-1})). \quad (6)$$

2.1 Additive properties of Fibonacci numbers

Theorem 2 finds application on additive problems for well known very fast increasing sequences. For example the following theorems on additive properties of the Fibonacci sequence $\{F_n\}$.

Theorem 4. *For $\pi(N)(1 + o(1))$ primes $p \leq N$, every integer λ can be written as*

$$F_{n_1} + \dots + F_{n_{16}} \equiv \lambda \pmod{p},$$

where $1 \leq n_1, \dots, n_{16} \leq N^{1/2+o(1)}$.

This improves the result of García, Luca and Mejía [10] on the representation of any residue class λ in the form

$$F_{n_1} + \dots + F_{n_{32}} \equiv \lambda \pmod{p},$$

for certain integers n_1, \dots, n_{32} , for almost all primes p . Moreover, combining Theorem 2 with exponential sum techniques we obtain a more general result.

Theorem 5. *Let $0 < \varepsilon < 1/2$. There is an integer $s < 100/\varepsilon$ such that for $\pi(N)(1 + o(1))$ primes $p \leq N$, every integer λ can be written as*

$$F_{n_1} + \dots + F_{n_s} \equiv \lambda \pmod{p},$$

where $n_i \leq N^\varepsilon$, $i = 1, \dots, s$.

Observe that the number of terms on the sumatory has the expected order, apart from the value 100. Indeed we obtain $s = 4(\lceil 8/\varepsilon \rceil - 1)$. However, we do not consider a reduction to be essential in this paper.

2.2 Application to the discrete Littlewood problem

The following theorem presents an application of a result of Bourgain and Garaev [4, Theorem 1.4].

Theorem 6. *Let g be a primitive root modulo p . If $N < p^{1/2}$ then*

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right| \gg N^{1/48+o(1)}.$$

Regarding the Fibonacci sequence, we prove the following theorem.

Theorem 7. *Let $0 < \gamma < 1/3$. There are two positive absolute constants $c_1 = c_1(\gamma)$, $c_2 = c_2(\gamma)$ such that for $\pi(N)(1 + o(1))$ primes, $p \leq N$, we have*

$$c_1 N^{\gamma/2} \leq \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \leq c_2 N^{\gamma/2}.$$

3 Notation and lemmas

For given subsets \mathcal{A} and \mathcal{B} of the residue field \mathbb{F}_p and any integer $k \geq 2$, as usual, we denote

$$\begin{aligned} \mathcal{A} + \mathcal{B} &= \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}, \\ \mathcal{A} \cdot \mathcal{B} &= \{ab : a \in \mathcal{A}, b \in \mathcal{B}\}, \\ k\mathcal{A} &= \{a_1 + \dots + a_k : a_1, \dots, a_k \in \mathcal{A}\}. \end{aligned}$$

For any finite subset of integers \mathcal{X} we denote

$$\mathcal{X} \pmod{p} = \{x \pmod{p} : x \in \mathcal{X}\}.$$

The next lemma is a result of Glibichuk [11].

Lemma 8. *Let \mathcal{A}, \mathcal{B} be subsets of \mathbb{F}_p such that $|\mathcal{A}||\mathcal{B}| > 2p$. Then*

$$8\mathcal{A} \cdot \mathcal{B} = \mathbb{F}_p. \quad \square$$

Given a fixed prime number p , we denote by t_p the *multiplicative order* of 2 modulo p . That is

$$t_p = \min\{\ell : 2^\ell \equiv 1 \pmod{p}\}.$$

As we mentioned in the introduction, the result of Erdős–Murty [5] establish that for $\pi(N)(1 + o(1))$ primes, $p \leq N$, we have $t_p > N^{1/2} e^{(\log N)^{\rho_0}}$, with some sufficiently small $\rho_0 > 0$. We present an analogous result for the *order of appearance*, defined by

$$z(k) = \min\{\ell : F_\ell \equiv 0 \pmod{k}\},$$

where k is a fixed integer $k \geq 2$ and F_n denotes the n th term of the sequence of Fibonacci numbers.

Lemma 9. *For almost all primes $p \leq N$, we have*

$$z(p) \geq N^{1/2} e^{(\log N)^\rho},$$

with some appropriate $\rho > 0$.

We require the following lemma which follows from exponential sums estimates, see for example the proof of [8, Theorem 1.1] or [17].

Lemma 10. *Let X, Y and Z be subsets of $\{0, 1, \dots, p-1\}$. Denote by T the number of solutions of the congruence*

$$xy + z_1 + z_2 \equiv \lambda \pmod{p}, \quad (7)$$

where

$$x \in X, \quad y \in Y, \quad z_1, z_2 \in Z.$$

Then, the asymptotic formula

$$T = \frac{|X||Y||Z|^2}{p} + \theta \sqrt{p|X||Y||Z|}, \quad |\theta| \leq 1,$$

holds uniformly over λ . In particular Eq. (7) has solution if $|X||Y||Z|^2 > p^3$.

We shall use some results concernig the values of Fibonacci sequence.

$$F_{u+v} = \frac{1}{2}(F_u L_v + L_u F_v), \quad (8)$$

$$F_{u-v} = \frac{(-1)^v}{2}(F_u L_v - L_u F_v), \quad (9)$$

where $\{L_m\}$ is the Lucas sequence given by

$$L_{m+2} = L_{m+1} + L_m, \quad L_1 = 1, L_2 = 3.$$

The following lemma is due to Bourgain and Garaev [4]

Lemma 11. *Let g be a fixed primitive root modulo p . Let $1 < M < p^{1/2}$ and denote by T be the number of solutions of the congruence*

$$g^x + g^y \equiv g^z + g^w \pmod{p}; \quad 1 \leq x, y, z, w \leq M.$$

Then

$$T < M^{3-1/24+o(1)}.$$

4 Proof of Theorems

4.1 Proof of Theorem 1

If $x = y$ then Eq. (3) has $\pi(N)|\mathcal{X}|$ solutions. Therefore

$$\mathcal{J}(N) = \pi(N)|\mathcal{X}| + \mathcal{J}', \quad (10)$$

where \mathcal{J}' denotes the number of solutions of (3) subject to $x \neq y$. Given x, y in \mathcal{X} with $x \neq y$, the equation

$$pk = x - y, \quad p \leq N,$$

has at most $\omega(|x - y|)$ solutions, where $\omega(n)$ denotes the number of prime divisors of n . If $4 \leq |x - y| \leq 10^M$, using the well-known estimate $\omega(n) \ll (\log n)/(\log \log n)$, we obtain that (3) has at most $\mathcal{O}(|\mathcal{X}|^2 M / \log M)$ solutions. Otherwise, if $0 < |x - y| < 4$, then (3) has no more than $\mathcal{O}(|\mathcal{X}|)$ solutions. Thus

$$\mathcal{J}' \ll |\mathcal{X}|^2 \frac{M}{\log M}.$$

Inserting this upper bound for \mathcal{J}' in (10), Theorem 1 follows. \square

4.2 Proof of Theorem 2

Before the proof, we shall introduce the following lemma

Lemma 12. *Let J_p be the number of solutions of the congruence*

$$x \equiv y \pmod{p}; \quad x, y \in \mathcal{X}. \quad (11)$$

For $\pi(n) = (1 + \mathcal{O}(1/\Delta))$ primes $p \leq N$ we have

$$J_p = |\mathcal{X}| + \mathcal{O}\left(\frac{|\mathcal{X}|^2 M}{\pi(N) \log M} \Delta\right). \quad (12)$$

Proof. Note that $J_p \geq |\mathcal{X}|$, because the case $x = y$ satisfies (11). It is clear that

$$\mathcal{J}(N) = \sum_{p \leq N} J_p.$$

Denote by \mathcal{P} the set of prime numbers $p \leq N$ such that

$$J_p - |\mathcal{X}| > \frac{|\mathcal{X}|^2 M}{\pi(N) \log M} \Delta.$$

If p runs through the set \mathcal{P} , recalling that $J_p - |\mathcal{X}| \geq 0$, we get

$$|\mathcal{P}| \frac{|\mathcal{X}|^2 M}{\pi(N) \log M} \Delta \leq \sum_{p \in \mathcal{P}} (J_p - |\mathcal{X}|) \leq \sum_{p \leq N} (J_p - |\mathcal{X}|) = \mathcal{J}(N) - \pi(N)|\mathcal{X}|.$$

Thus, applying Theorem 1, we derive that

$$|\mathcal{P}| \ll \frac{\pi(N)}{\Delta}.$$

Therefore, if \mathcal{Q} denotes the number of primes $p \leq N$ such that

$$J_p - |\mathcal{X}| \leq \frac{|\mathcal{X}|^2 M}{\pi(N) \log M} \Delta,$$

then

$$|\mathcal{Q}| = \pi(N) - |\mathcal{P}| = \pi(N)(1 + \mathcal{O}(\Delta^{-1})).$$

□

Theorem 2 follows from the relation

$$\#\{x \pmod{p} : x \in \mathcal{X}\} \geq \frac{|\mathcal{X}|^2}{J_p}. \quad \square$$

4.3 Proof of Theorem 4

Lemma 9 allow us to establish the order of the value set of the Fibonacci sequence for most primes

$$\#\{F_n \pmod{p} : n \leq \delta N^{1/2}\} \asymp \delta N^{1/2},$$

where $\delta = \delta(N) = e^{(\log N)^\rho}$ and $\rho > 0$ is the referred constant in Lemma 9. In order to establish the last relation, it is sufficient to prove that for

$$\mathcal{F} = \{F_{2n} : \delta N^{1/2}/10 < n \leq \delta N^{1/2}/5\},$$

we have

$$|\mathcal{F} \pmod{p}| = |\mathcal{F}| = \frac{\delta N^{1/2}}{10} + \mathcal{O}(1). \quad (13)$$

Let n, n' be positive integers such that

$$F_{2n} \equiv F_{2n'} \pmod{p}; \quad \delta N^{1/2}/10 < n, n' \leq \delta N^{1/2}/5. \quad (14)$$

Without loss of generality we can assume that $n \geq n'$. Substituting $u = n + n'$ and $v = n - n'$ in (8) and (9), we can obtain

$$F_{2n} - F_{2n'} = \frac{1}{2} \left((1 - (-1)^{n-n'}) F_{n+n'} L_{n-n'} + (1 + (-1)^{n-n'}) L_{n+n'} F_{n-n'} \right).$$

Suppose that $n - n' \equiv 0 \pmod{2}$, then from Eq. (14) follows

$$p | L_{n+n'} F_{n-n'}.$$

If $n \neq n'$, then $0 < n - n' < N^{1/2} \delta \leq z(p)$, which implies $(p, F_{n-n'}) = 1$. Thus

$$p | L_{n+n'}, \quad \text{in particular } p | F_{n+n'} L_{n+n'},$$

where $F_{n+n'}L_{n+n'} = F_{2(n+n')}$. Hence $p|F_{2(n+n')}$, with $2(n+n') < z(p)$. This contradicts the choice of $z(p)$. Therefore in the case $n - n' \equiv 0 \pmod{2}$ Eq. (14) has only trivial solutions $n = n'$. Similarly, it is possible to verify that (14) has not solutions if $n - n' \equiv 1 \pmod{2}$.

Now, consider the subset of Lucas sequence

$$\mathcal{L} = \{L_{2m} : 1 \leq m \leq N^{1/2}/\sqrt{\delta}\}.$$

Taking in Theorem 2; $M = N^{1/2}/\sqrt{\delta}$ and $\Delta = \delta^{1/4}$ we obtain

$$|\mathcal{L} \pmod{p}| = \frac{N^{1/2}}{\sqrt{\delta}}(1 + \mathcal{O}(\delta^{-1/4})). \quad (15)$$

Observe that equalities (13) and (15) are valid respectively for most primes. Thus, for $\pi(N)(1 + o(1))$ primes $p \leq N$ we have

$$|\mathcal{F} \pmod{p}| |\mathcal{L} \pmod{p}| \gg \sqrt{\delta}N \geq 2p.$$

Applying Lemma 8, we obtain that for almost all primes p every integer λ can be written as

$$F_{2n_1}L_{2m_1} + \dots + F_{2n_8}L_{2m_8} \equiv \lambda \pmod{p},$$

where

$$N^{1/2}\delta/10 < n_i \leq N^{1/2}\delta/5, \quad 1 \leq m_i \leq N^{1/2}/\sqrt{\delta}, \quad 1 \leq i \leq 8.$$

Using the identity

$$F_u L_v = F_{u+v} + (-1)^v F_{u-v},$$

for every $1 \leq i \leq 8$ we get

$$F_{2n_i}L_{2m_i} = F_{2(n_i+m_i)} + F_{2(n_i-m_i)}.$$

Thus, Theorem 4 follows. \square

4.4 Proof of Theorem 5

Let k be the minimal integer such that $1/(k+2) < \varepsilon/8$. Define the sets

$$X = \{F_{2n_1-1} + \dots + F_{2n_k-1} : 1 \leq n_1, \dots, n_k \leq N^{\frac{1}{k+2}}\},$$

$$Y = \{L_m : \frac{1}{2}N^{\frac{7}{k+2}} < m \leq N^{\frac{7}{k+2}}\},$$

$$Z = \{F_{2\ell_1} + \dots + F_{2\ell_k} : 1 \leq \ell_1, \dots, \ell_k \leq N^{\frac{1}{k+2}}\}.$$

Observe that $|Y| \gg N^{\frac{7}{k+2}}$ and exist a positive constant $c = c(k) < 1$ such that

$$|X|, |Z| \geq cN^{\frac{k}{k+2}}.$$

In order to estimate the value set of $X \pmod{p}$ note that if $x \in X$, then $x \leq 10^{\log k N^{1/(k+2)}}$. Thus, applying Corollary 3 with $M = \log k N^{1/(k+2)}$, $\mathcal{X} = Z$ and $\Delta = (\log N)^A$, (for any integer $A > 0$), we have that for most of primes $p \leq N$

$$|X \pmod{p}| = |X|(1 + o(1)).$$

Analogously, we can obtain

$$|Y \pmod{p}| = |Y|(1 + o(1)), \quad |Z \pmod{p}| = |Z|(1 + o(1)),$$

for almost all primes respectively. Therefore, there is a constant $c_1 = c_1(k)$, $0 < c_1 < 1$, such that for $\pi(N)(1 + o(1))$ primes $p \leq N$ we have

$$|X \pmod{p}| |Y \pmod{p}| |Z \pmod{p}|^2 \geq c_1 N^{3 + \frac{1}{k+2}} > p^{3 + \frac{1}{k+2}}.$$

Applying Lemma 10 it follows that for almost all primes every integer λ can be represented as

$$\sum_{i=1}^k L_m F_{2n_i-1} + \sum_{j=1}^k (F_{2\ell_j} + F_{2\ell'_j}) \equiv \lambda \pmod{p}, \quad (16)$$

where

$$\frac{1}{2} N^{\frac{7}{k+2}} < m \leq N^{\frac{7}{k+2}}, \quad 1 \leq n_i \leq N^{\frac{1}{k+2}}, \quad 1 \leq \ell_j, \ell'_j \leq N^{\frac{1}{k+2}}, \quad (1 \leq i, j \leq k).$$

We recall the identity

$$L_u F_v = F_{u+v} + (-1)^{v+1} F_{u-v}.$$

Thus, for every $1 \leq i \leq k$ in (16) we get

$$L_m F_{2n_i-1} = F_{m+2n_i-1} + F_{m-2n_i+1}.$$

taking $s = 4k$ (that is, $s = 4(\lceil 8/\varepsilon \rceil - 1)$), we conclude that for almost all primes every residue class λ has a representation in the form

$$F_{n_1} + \dots + F_{n_s} \equiv \lambda \pmod{p},$$

for some integers

$$1 \leq n_1, \dots, n_s \leq N^\varepsilon. \quad \square$$

4.5 Proof of Theorem 6

Note that the congruence

$$g^x \equiv g^y \pmod{p}; \quad 1 \leq x, y \leq N,$$

has exactly N solutions. Therefore,

$$N = \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right|^2 = \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right|^{2/3} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right|^{4/3},$$

using Hölder's inequality we obtain

$$\begin{aligned} N &\leq \frac{1}{p} \left(\sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right| \right)^{2/3} \left(\sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right|^4 \right)^{1/3} \\ &\leq T^{1/3} \left(\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right| \right)^{2/3}, \end{aligned}$$

where, T denotes the number of solutions of the congruence

$$g^x + g^y \equiv g^z + g^w \pmod{p}; \quad 1 \leq x, y, z, w \leq N.$$

Thus, from Lemma 11 we know that $T < N^{3-1/24+o(1)}$. Therefore

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N} e^{2\pi i \frac{x}{p} g^n} \right| > N^{1/48-o(1)}. \quad \square$$

4.6 Proof of Theorem 7

Observe that the congruence

$$F_n \equiv F_{n'} \pmod{p}; \quad 1 \leq n, n' \leq N^\gamma,$$

has at least N^γ solutions. Therefore

$$N^\gamma \leq \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right|^2.$$

From Hölder's inequality, as in the proof of Theorem 6, it is possible to obtain

$$N^\gamma \leq T_p^{1/3} \left(\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \right)^{2/3}, \quad (17)$$

where T_p denotes the number of solutions of the congruence

$$F_{n_1} + F_{n_2} \equiv F_{m_1} + F_{m_2} \pmod{p}; \quad 1 \leq n_1, n_2, m_1, m_2 \leq N^\gamma.$$

Let

$$\mathcal{X} = \{F_{n_1} + F_{n_2} : 1 \leq n_1, n_2 \leq N^\gamma\}.$$

Then $|\mathcal{X}| \asymp N^{2\gamma}$. Applying Lemma 12 with $M = N^\gamma$ and $\Delta = N^{(1-3\gamma)/2}$ we get, for $\pi(N)(1 + o(1))$ primes $p \leq N$, the estimation

$$T_p \leq N^{2\gamma} \left(1 + N^{-(1-3\gamma)/2}\right).$$

Combining this estimation with relation (17) we conclude that there is a positive constant $c_1(\gamma)$ such that

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \geq c_1(\gamma) N^{\gamma/2}.$$

Finally, to obtain an upper bound of the same order, using the Cauchy-Schwartz inequality we have

$$\left(\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \right)^2 \leq \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right|^2, \quad (18)$$

where the right term is, indeed, the number of solutions of the congruence

$$F_n \equiv F_m \pmod{p}; \quad 1 \leq n, m \leq N^\gamma.$$

Applying again Lemma 12 with $M = N^\gamma$ and $\Delta = N^{(1-2\gamma)/2}$, we obtain, for $\pi(N)(1 + o(1))$ primes $p \leq N$, the estimation

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right|^2 \leq N^\gamma \left(1 + N^{-(1-2\gamma)/2}\right) \leq c_2(\gamma) N^\gamma,$$

for some positive constant $c_2(\gamma)$. Putting together with (18) and taking square root we conclude the proof. \square

References

- [1] W. D. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, ‘Exponential sums over Mersenne numbers,’ *Compos. Math.*, **140** (1), 15–30 (2004).
- [2] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, ‘Uniform distribution of fractional parts related to pseudoprimes,’ *Canad. J. Math.*, **61** (3), 481–502 (2009).
- [3] J. Bourgain, ‘Estimates on exponential sums related to the Diffie–Hellman distributions,’ *Geom. Funct. Anal.*, **15** (1), 1–34 (2005).
- [4] J. Bourgain, M. Z. Garaev, ‘On a variant of sum-product estimates and explicit exponential sum bounds in prime fields,’ *Math. Proc. Cambridge Philos. Soc.*, **146** (1), 1–21 (2009).

- [5] P. Erdős and M. R. Murty, ‘On the order of $a \pmod{p}$ ’, in *Number theory (Ottawa, ON, 1996)*, 87–97, CRM Proc. Lecture Notes **19**, Amer. Math. Soc., Providence, RI, 1999.
- [6] M. Z. Garaev, ‘Upper bounds for the number of solutions of a diophantine equation,’ *Trans. Amer. Math. Soc.*, **357**, 2527–2534 (2005).
- [7] M. Z. Garaev, ‘The large sieve inequality for the exponential sequence $\lambda^{[O(n^{15/14+o(1)})]}$ modulo primes’ *Canad. J. Math.*, **61** (2), 336–350 (2009).
- [8] M. Z. Garaev and Ka-Lam Kueh, ‘Distribution of special sequences modulo a large prime’ *Int. J. Math. Math. Sci.*, **50**, 3189–3194 (2003).
- [9] M. Z. Garaev and I. E. Shparlinski, ‘The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes,’ *Int. Math. Res. Notices*, (39), 2391–2408 (2005).
- [10] V. C. Garcia, F. Luca and V. J. Mejia, ‘On sums of Fibonacci numbers modulo p ,’ *Bull. Aust. Math. Soc.*, (to appear).
- [11] A. A. Glibichuk, ‘Combinatorial properties of sets of residues modulo a prime an the Erdős–Graham problem’, *Mat. Zametki* **79**:3, 384–395 (2006); English transl., *Math. Notes* **79**:3–4, 356–365 (2006).
- [12] B. Green and S. V. Konyagin, ‘On the Littlewood problem modulo a prime,’ *Canad. J. Math.* **61** (1), 141–164 (2009).
- [13] A. A. Karatsuba, ‘An estimate of the L_1 -norm of an exponential sum,’ *Math. Notes*, **64**, 401–404 (1998).
- [14] S. V. Konyagin, ‘On the problem of Littlewood,’ *Izv. Acad. Nauk SSSR Ser. Mat. [Math. USSR-Izv.]*, **45** (2), 243–265 (1981).
- [15] S. V. Konyagin, ‘An estimate of the L_1 -norm of an exponential sum,’ *The Theory of Approximations of Functions and Operators. Abstracts of Papers of the International Conference Dedicated to Stechkins 80th Anniversary [in Russian]*. Ekaterinburg (2000), pp. 88–89.
- [16] O. C. McGehee, L. Pigno and B. Smith, ‘Hardy’s inequality and the L_1 norm of exponential sums,’ *Ann. of Math.* (2), **113**(3), 613–618 (1981).
- [17] A. Sárközy, ‘On sums and products of residues modulo p ,’ *Acta Arith.*, **118** (4), 403–409 (2005).